"The opinions or assertions contained herein are the private ones of the speaker and are not to be construed as official or reflecting the views of the Department of Defense or the Office of the Inspector General."

Building Strong Control Environments through Risk Management

(*Update on Purchase Card Systemic Weakness)*

COL William J. Kelley CISA, CISM

For Official Use Only

IG Mission

Achievement

The OIG Mission Endeavors To:

"Encourage a culture of creativity and intelligent risk taking;"

"Foster and promote public accountability and integrity"

"Provide leadership…to promote economy, efficiency and effectiveness";

Prevent and detect "waste, fraud and abuse";

Keep the Secretary of Defense and Congress "fully and currently informed;" and

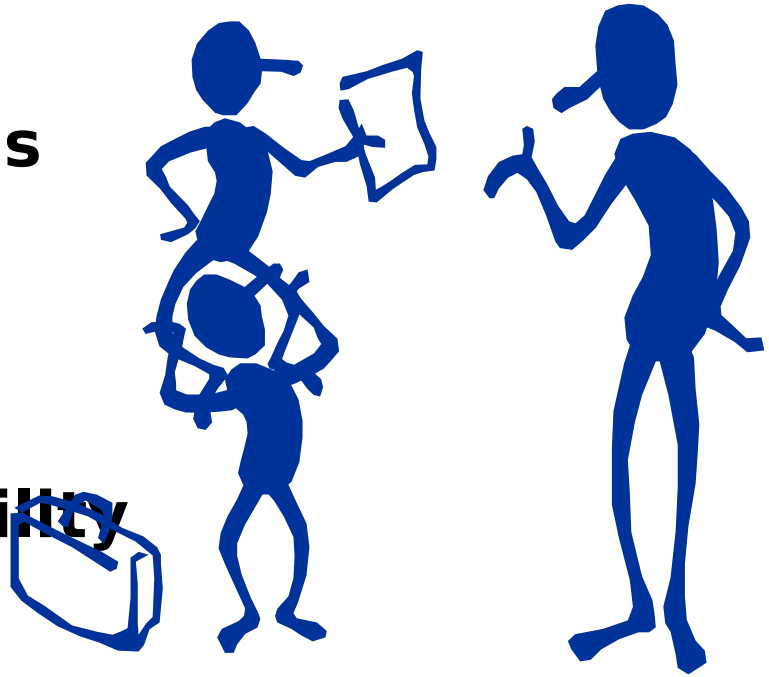
"avoiding duplication and insuring effective coordination and cooperation."

OIG Vision

We reflect and promote excellence in the Department of Defense.

Congressional Interest

- **Headline Grabbing Items**
- **Constituency Interest**
- **Government Accountability**
- **Recent Testimony**



Senate Governmental Affairs ommittee Testimony – 28 April 2004

"In Fiscal Year 2003, the Department made 10.7 million purchase actions valued at about $7.2 billion. Every working day DoD employees make about 41,000 purchases valued at $27.6 million. A day's worth of purchase receipts could make a pile that stands over 13 feet tall. We need to build processes that pick the most important receipts from that pile to review because we can't review them all. Management oversight we think would include one process that would restack those receipts based on risk. That risk could be identifying receipts that were for services or items that were potentially unneeded or wasteful."

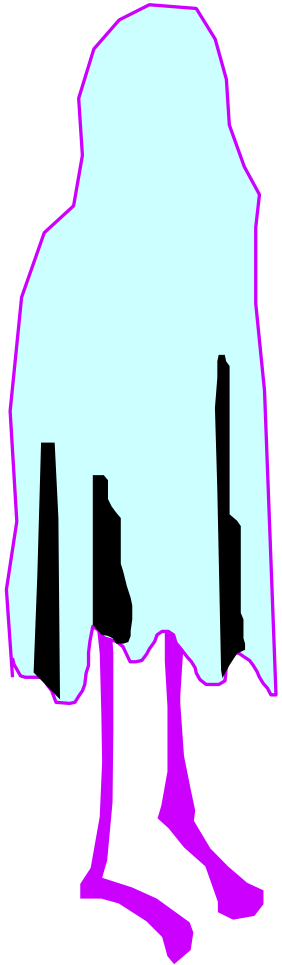
-- Colonel William J. Kelley, USA


Need to Study
And Perform
DATA
Continuous

Risks Concepts

- Risks are those activities that could impede the efficient and effective accomplishment of objectives
- Risks are identified and assessed for relevance
- Risks are analyzed for significance
- Controls are then selected to mitigate significant risks
- Controls must be periodically tested to ensure that they are in place and working

SEVENTH ATTRIBUTE OF *MOST* FRAUDS



- **Perpetrator**
- **Victim**
- **Motive**
- **Opportunity**
- **Intent**
- **Scenario (*Modus Operandi*)**
- **CONCEALMENT**

For Official Use Only

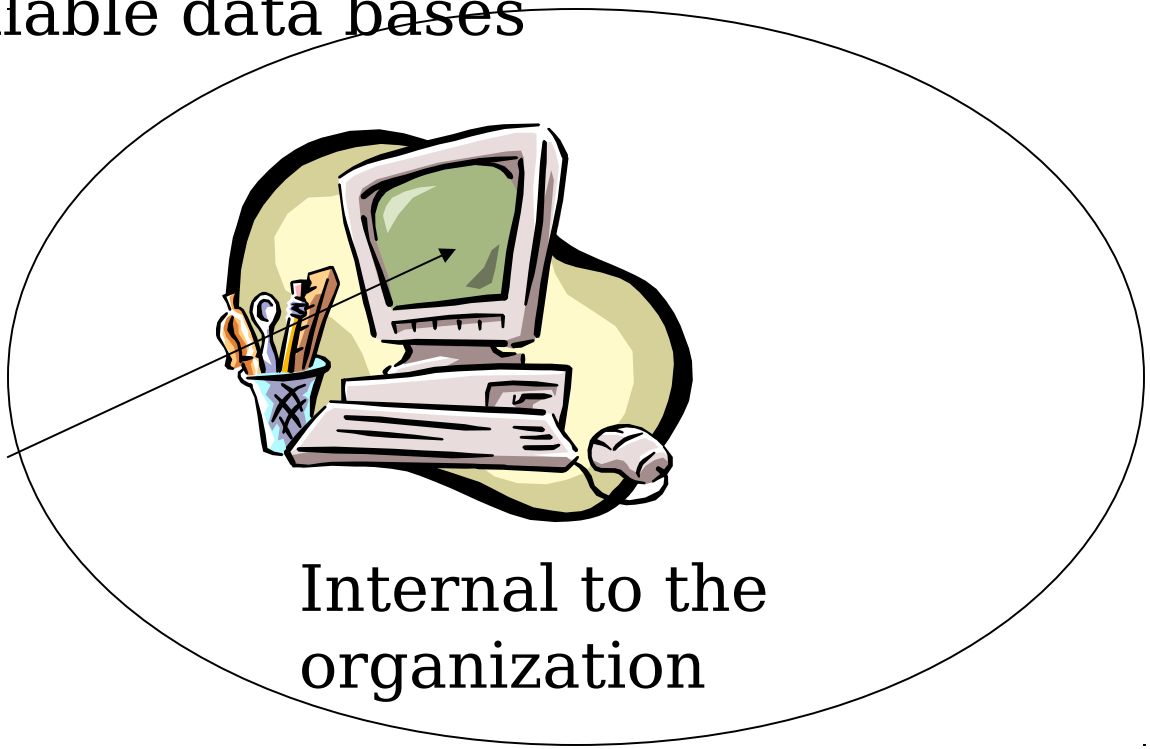
Purchase Card Problem Areas

Abuse and misuse includes a range of actions such as:

- Splitting procurements to avoid procurement thresholds
- Purchasing goods or services which, although for a valid governmental purpose, are prohibited on a purchase card
- Purchasing items for which there is no government need
- Purchasing items which do not represent best value to the government
- Engaging in fraudulent activity
- Invoices were being certified without being reviewed.

Data Analysis – A Generic Approach

Identify all available data bases

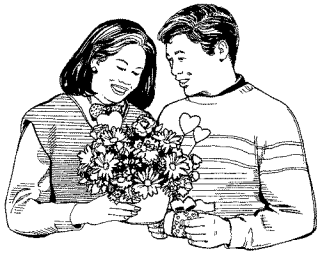


Internal to the organization

External to the organization

List record fields in all available databases

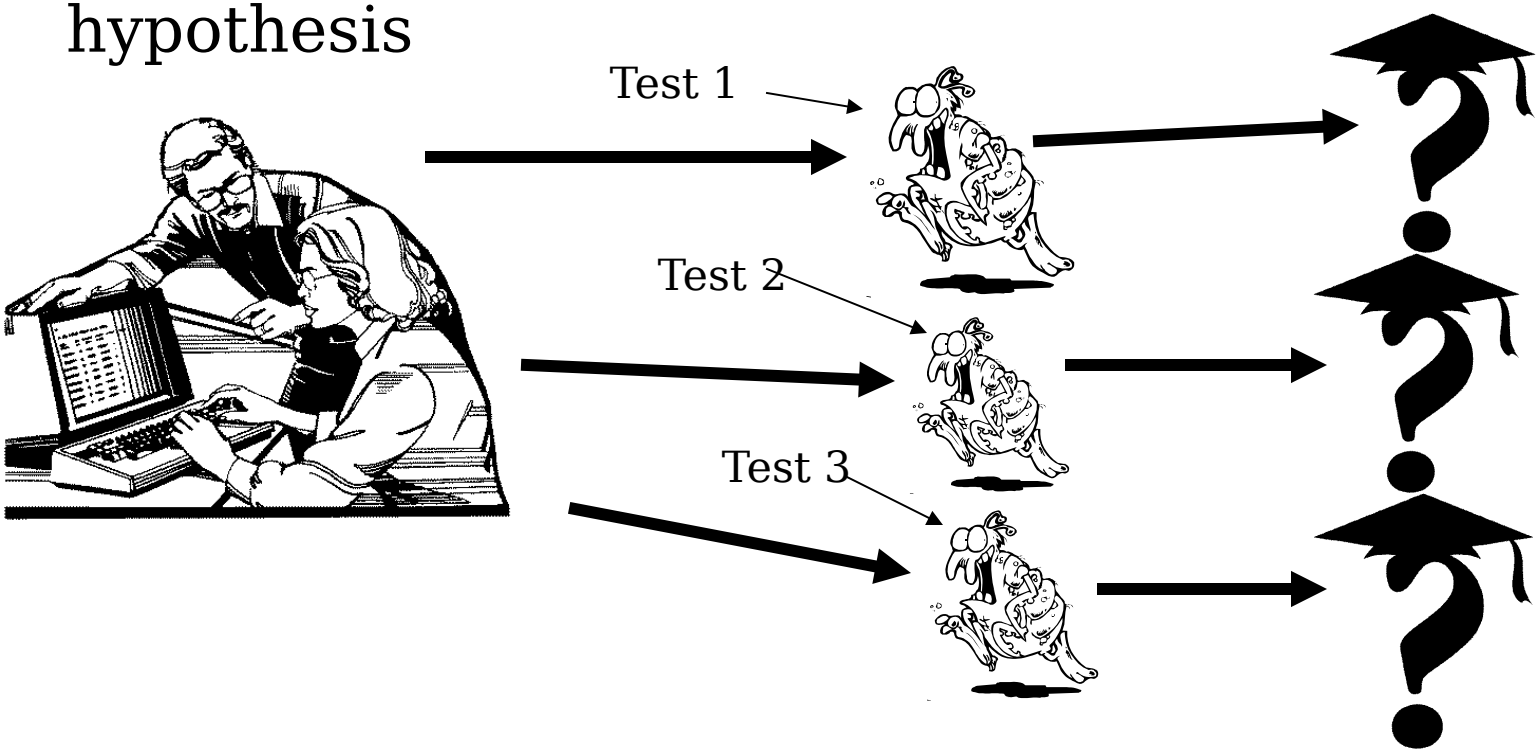
Formulate hypotheses about record field relationships



Possible Tests for High Risk Card Holders

1. Does the transaction fall within a suspicious/unusual merchant category code?
2. Does the cardholder have transactions (authorizations) occurring on non-working days (e.g. weekends)?
3. Is the vendor being used by only a limited number of cardholders?

Program analytical tests for each hypothesis



Test 1 2 3

Run tests (output is your “hit list”)

Possible Tests for High Risk Card Holders

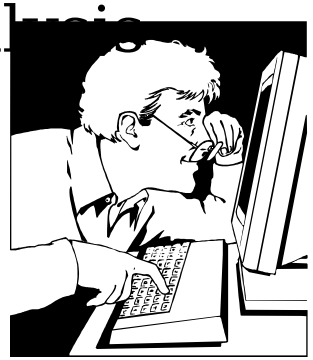
1. Has the account been closed due to fraud and a new card reissued?
2. Has the cardholder allowed others in the office to use their card for making purchases?
3. Does the cardholder repeatedly do business with the same merchants (minimal rotation)?

Evaluate initial hit list and refine the tests

Re-run refined test to produce shorter, more meaningful hit list (repeat steps 5-7, as needed)

Evaluate (via record analysis, interview, or other technique) every item on the refined hit list.

Record Analysis



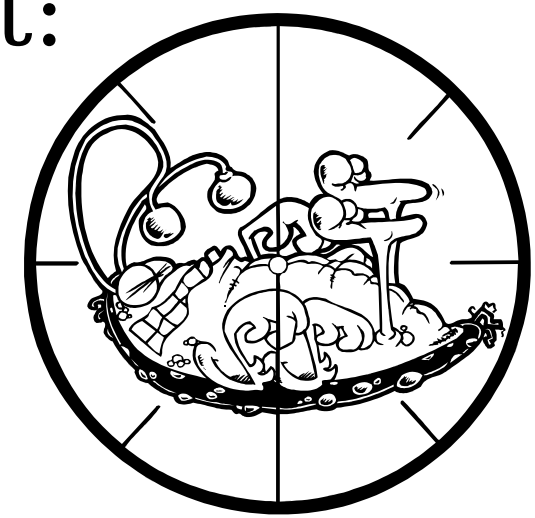
Interview

Other technique

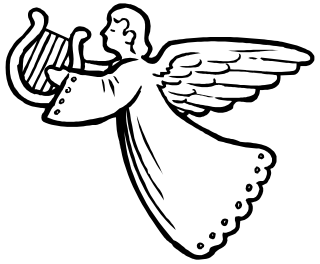
Possible Tests for igh Risk Card Holders

1. Is the cardholder unable to provide proof of purchase such as receipts?
2. Do the items purchased meet a bona fide government need?

Dispose of every hit:



Valid Explanation found or misuse not fraud



Probable improper transaction – full investigation needed

Identify control problems and corrective actions needed

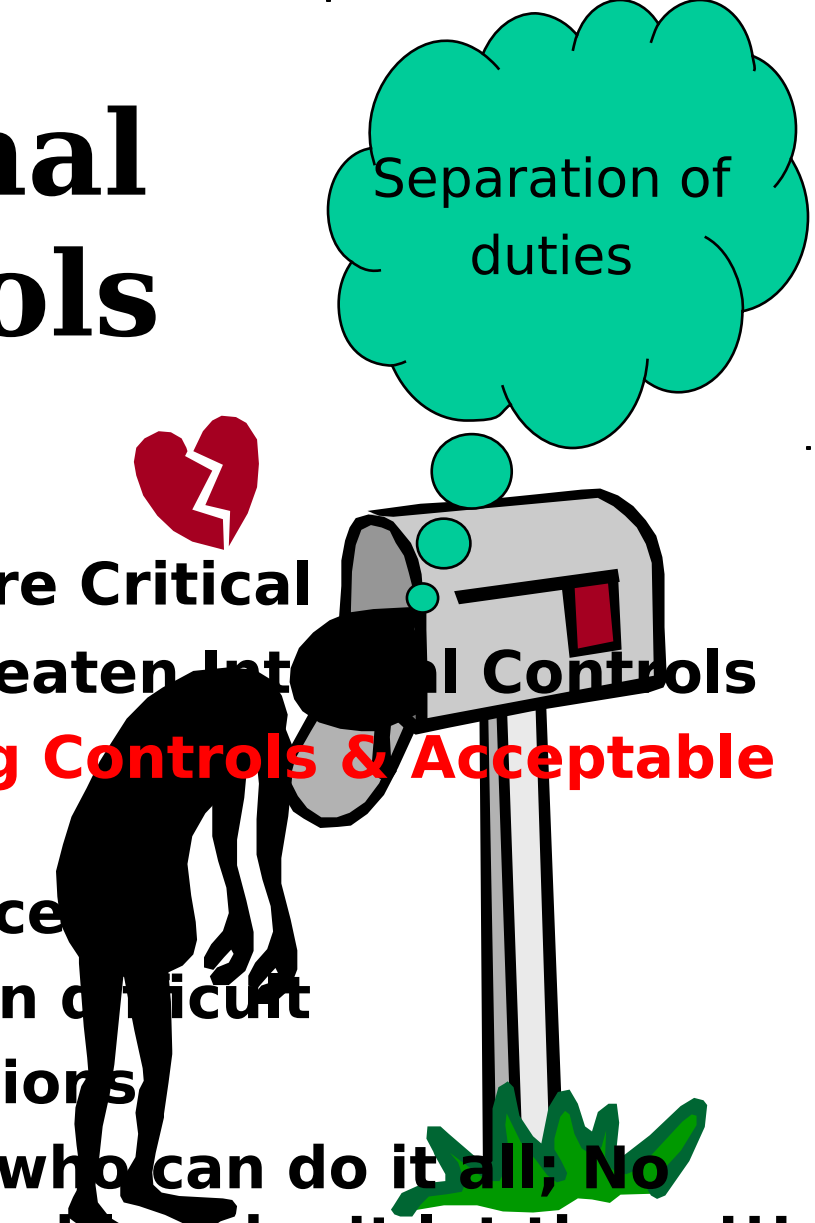
Control Problems

Corrective Actions Needed

Watch For Anomalies

- **Missing Documents**
- **Photocopies**
- **Unreturned Confirmations**
- **Unsupported or Unapproved Adjustments**
- **Missing approval signatures**
- **Unusual Number of Disputes**
- **Unreconciled accounts; missing canceled checks**
- **Unusual refund activity**
- **Missing property records**
- **When the Data is too *perfect***

Internal Controls



- **Good Internal Controls are Critical**
- **Dwindling Resources Threaten Internal Controls**
- **Remember Compensating Controls & Acceptable Level of Risk**
- **Passwords & Systems Access**
- **Collusion makes detection difficult**
- **Enforce Mandatory Vacations**
- **Beware of the Employee who can do it all; No matter how capable - don't let them !!!**

Need for Data Mining

- During December 2001, OIG DoD, DFAS and the DoD Purchase Card Program Management Office agreed to develop a automated oversight program using data mining technology to identify purchase card transactions having a high probability of fraud or abuse.

Four General Categories

- Personal Purchases
- Cardholder Conspiracy With Vend
- Vendor Fraud
- External Fraud

These schemes can also be used in various combinations.

Fraud Indicators

- Regularly recurring split purchases, often to the same vendor
- Purchases outside normal purchase pattern of cardholder (possibly made by others)
- Recurring purchases from relatively unknown sources/vendors
- Purchased items not annotated on property books

Audit to Risk

tional Oversight – 100% manual review was not working

Can not do 11 million transactions a year

- Audit Focus
  - automated 100% review based on business rules
  - resulting in review of a percentage of the transactions with greatest risk.
- Audit Approach
  - create partnerships
    - DoD Program Management Office
    - General Accounting Office
    - Banking Vendors
    - Defense Finance and Accounting Service
    - Military Criminal Investigative Organizations
    - Other Defense Agency IGs and Internal Review Offices
    - OIG DoD
    - General Services Administration
    - Service Audit Agencies
- Reviewed 17,622 transactions related to 1,357 cardholders in 752 cities
- Identified 182 cardholders who expended about $20 million on potentially inappropriate/fraudulent transactions.

DoD GPC Statistics

	FY 2001	FY 2002	FY 2003	FY 2004
Total Sales	$6,106,028,852	$6,803,230,403	$7,184,887,175	$7,506,136,140
Number of Card Holders	202,720	214,099	141,092	172,942
Transactions	10,668,438	10,980,439	10,700,055	11,239,693

Project Purpose

- Create Partnership Between “Fraud Focus Group” And Service Investigative Organizations and Audit Agencies To Develop and Evaluate a Pilot Project For Automated Purchase Card Oversight
- Develop A Method To Identify Anomalies In Purchase Card Data That May Indicate Fraud Or Abuse
- Assess And Improve The Detection Process
- Incorporate Effective Indicators Into Purchase Card Process

Participating Organizations

- DoD Purchase Card Management Office
- OIG, DoD
  - Defense Criminal Investigative Service
  - Assistant Inspector General for Auditing
- Service Auditor Generals
- Military Criminal Investigative Organizatio
  - Naval Criminal Investigative Service
  - Air Force Office of Special Investigations
  - Army Criminal Investigation Command
- Defense Finance And Accounting Service (DFAS), Internal Review
- Defense Manpower Data Center (DMDC)
- Other Defense Agency Inspector General and Internal Review Offices

Developing Indicator Combinations

- Few Single Indicators Are Effective
- Need to Reduce False Positives and Limit the Number of Card Holder Profiles
- Number of Possible Combinations is Staggering
- A Few of the Most Interesting Combinations Can Be Initially Selected and Evaluated
- Other Combinations Can Be Continuously Developed and Evaluated
- Highly Interesting Individual Transactions Are Also Identified During the Process of Evaluating Indicators

Examples of Activities Targeted by Data Mining

Indicators used to identify potential fraud or misuse

- Repetitive buying pattern of even dollars, near purchase limits, or same or similar name for vendor
- Name for merchant and cardholder (or approving official) the same
- Fewer than 5 cardholders using a specific vendor
- Purchases approved by cardholder or no specific person instead by a office

Examples of Indicators of Management Control Deficiencies

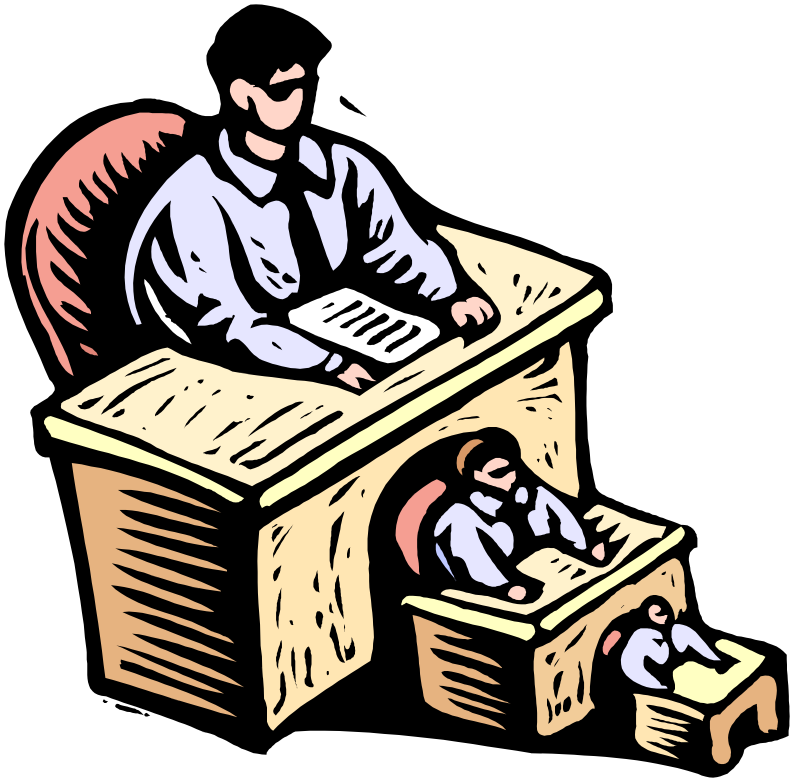
- Too many cards per Approving Official (AO) (management goal no more than 7 cardholders to an AO)
- Too many transactions per AO (management goal no more than 300 transactions to an AO)
- Card assigned to office or group of individuals instead of a specific person

Continuous Monitoring by Management

Prior Audits vs. Data-Mining Approach

PRIOR METHOD	CURRENT METHOD
- Manual inquiries for background documentation	- Automated e-mail and standard format with responses in database for data-mining
- Responses often vague in content and add little value	- Responses objective - Easier to query and track - Allow for Automated Analysis
- Transaction from 1 - 2 years ago	- Most recent month's transactions
- Top-down inquiries	- Bottom-up Reporting (Automated tool pushes reporting to AO)

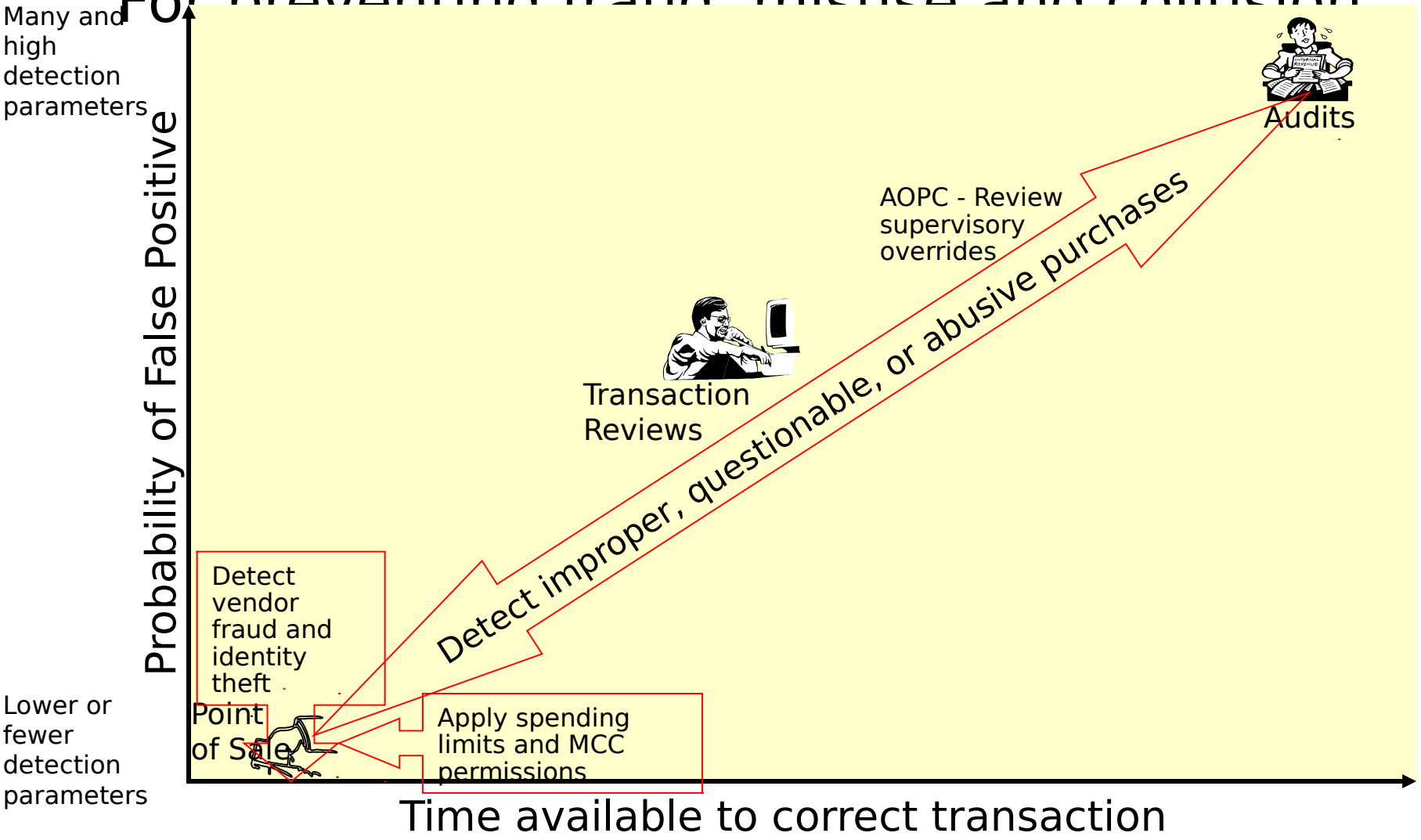
Goals for Continuous Monitoring



- Goals for DoD
- Goals for the services/ agencies
- Goals for the installations and units

Balancing Risk and Productivity

For preventing fraud, misuse and collusion

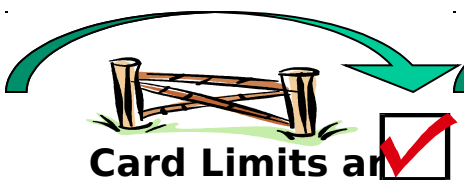


Purchase Card Defense in Depth

Point of Sale

Transaction Review

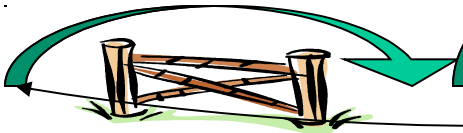
Audit



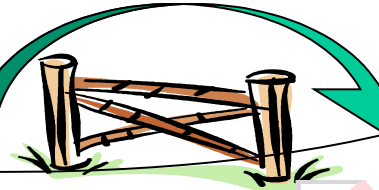
Card Limits and Merchant Focusing

Card Usage Profiling

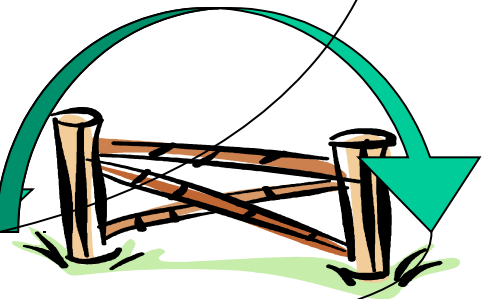
Defined Rules and Referral Process



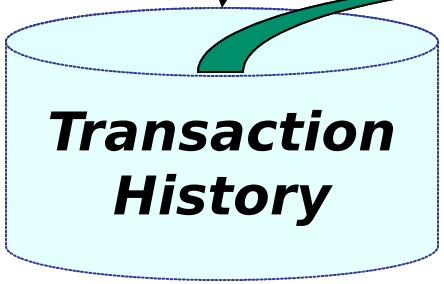
Cardholder Review

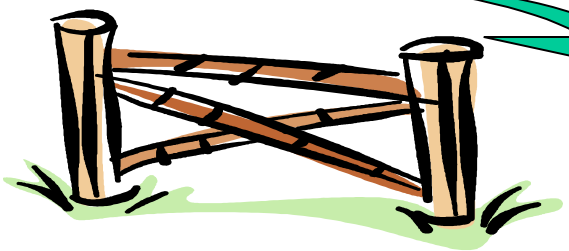


Rules Supported Supervisory Review



Rules Based Assisted Oversight

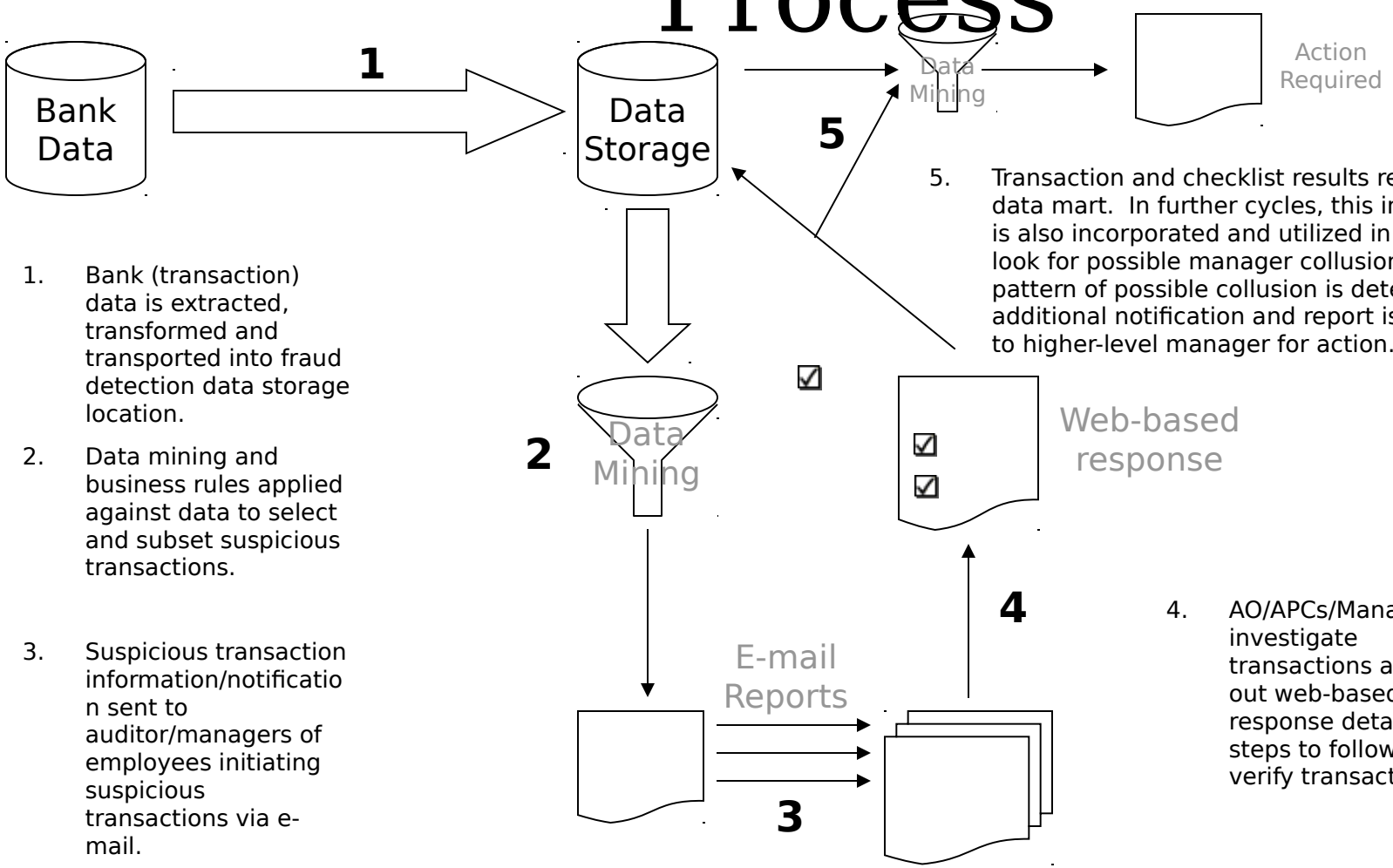




Post-Approval Sampling

Low Risk of Fraud or Misuse

A Continuous Monitoring Rules Process

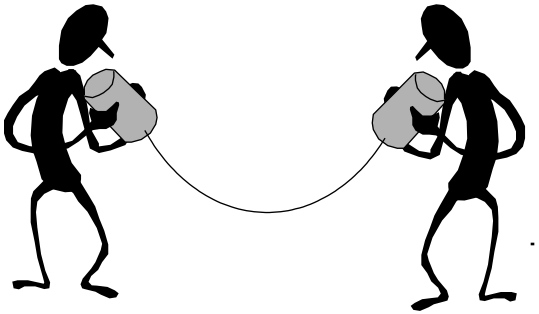


1. Bank (transaction) data is extracted, transformed and transported into fraud detection data storage location.
2. Data mining and business rules applied against data to select and subset suspicious transactions.
3. Suspicious transaction information/notification sent to auditor/managers of employees initiating suspicious transactions via e-mail.
4. AO/APCs/Managers investigate transactions and fills out web-based survey response detailing steps to follow to verify transaction.
5. Transaction and checklist results returned to data mart. In further cycles, this information is also incorporated and utilized in step 2 to look for possible manager collusion. If a pattern of possible collusion is detected, additional notification and report is submitted to higher-level manager for action.

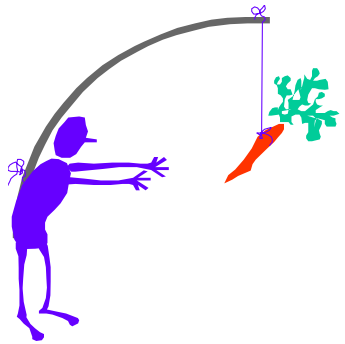
Other Federal Agencies

- PCIE dealing with erroneous payments
- Procurement Policy Analyst, Office of Federal Procurement Policy
- CIA Office of Inspector General Investigations Staff
- Commerce Inspector General
- DOJ OIG Fraud Detection Office
- Postal Service Office of Inspector General Investigations Staff
- Small Business Administration Office of Inspector General Investigations Staff
- U.S. Department of Justice, Federal Bureau of Prisons

Future of Data Mining/ Continuous Monitoring



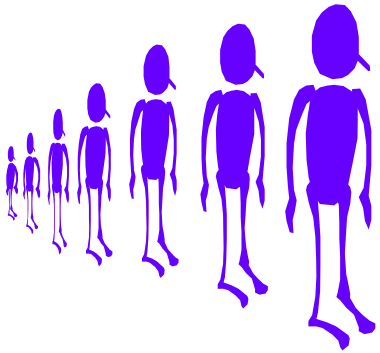
OIG DoD Auditors



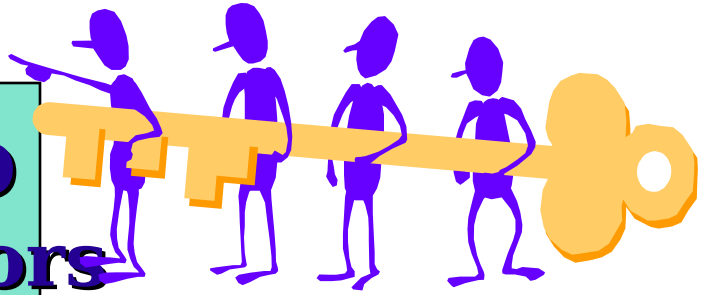
Military Criminal Investigative Organizations

Data

Service/Defense Agency Audit Organizations



OIG DoD Investigators



Current Projects/Audits

- Unauthorized and Questionable Purchases
  - Purchase Cards
  - Travel Cards
  - Communications Services, including long distance services, cellular phones and phone cards
  - Fleet Cards
  - AIR Cards
  - Contract Action Data Discrepancies
  - Power Track

Where to Get More Information

- *Application of Computer Assisted Audit Techniques Using Microcomputers*, Canadian Institute of Chartered Accountants, 1994 [www.isaca.org]
- *CAATTs & Other BEASTs for Auditors*, David G. Coderre, Global Audit Publications, 1998 [604/669-4225; or www.acl.com]
- *Fraud Detection: Using Data Analysis Techniques to Detect Fraud*, David G. Coderre, Global Audit Publications, 1999 [604/669-4225; or www.acl.com]

Where to Get More Information

- *101 ACL Applications: A Toolkit for Today's Auditors*, Richard B. Lanza, CPA, Global Audit Publications, 1999 [604/669-4225; or www.acl.com]
- About Benford's Law: *I've Got Your Number*, Mark J. Nigrini, Journal of Accountancy, May 1999
- About ACL: www.acl.com
- About IDEA: www.audimation.com

Where to Get More Information

- About Detective Toolkit, Fraud Investigator, and Similarity Search Engine: www.infoglide.com
- About ViCLAS: www.mtps.on.ca/Year/ViCLAS
- About Data Mining:
  - www.gartner6.gartnerweb.com
  - www.statserv.com/datamining.html
  - www.datamining.org/sites.htm
  - www.wizsoft.com
- About *Financial Crime Investigator*: www.cci2.com/fci_prod.htm

Resources

- www.itaudit.org
- **www.theiia.org**
- www.cica.org
- www.coso.org
- www.isaca.org
- www.aicpa.org
- Others?

Contact Information:

COLONEL Bill Kelley, CISA, CISM

(703) 604-9312

wkelley@dodig.osd.mil